Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Ley Sarbanes Oxley

🏛 Material de Estudio

Presentación del tema

La **Ley Sarbanes-Oxley**, conocida como **SOX (Sarbanes-Oxley Act – Ley Sarbanes-Oxley)**, es una normativa estadounidense promulgada en 2002 con el objetivo de **fortalecer la transparencia, la confiabilidad de la información financiera y los controles internos** de las organizaciones que cotizan en bolsa en los Estados Unidos. Si bien su origen está vinculado a escándalos financieros y contables, su impacto es especialmente significativo en el ámbito de los **Sistemas y Tecnologías de la Información (TI)**, ya que gran parte de la información financiera se **genera, procesa, almacena y reporta a través de sistemas informáticos**.

Desde la perspectiva de la administración, SOX transforma a los sistemas de información en **componentes críticos del control interno**, imponiendo responsabilidades claras sobre la forma en que se gestionan los datos, los accesos, los cambios en los sistemas y la trazabilidad de la información financiera. Comprender SOX desde TI implica reconocer que **la tecnología no solo soporta el negocio, sino que también puede convertirse en una fuente de riesgo regulatorio si no se gestiona adecuadamente**.

Desarrollo

1. ¿Qué es Sarbanes-Oxley y cuál es su objetivo principal?

La **Sarbanes-Oxley Act (SOX)** establece un marco legal destinado a:

- Proteger a los inversores.
- Asegurar la confiabilidad de los estados financieros.
- Reforzar la responsabilidad de la alta dirección.
- Exigir controles internos efectivos.

Desde los sistemas de información, SOX parte de un supuesto central:

> si los sistemas que procesan información financiera no son confiables, la información contable tampoco lo será.

Por este motivo, la ley no se limita a controles contables tradicionales, sino que exige **controles sobre los procesos tecnológicos** que intervienen en la generación de información financiera.

---

2. Relación entre SOX y los Sistemas de Información

Los sistemas de información desempeñan un rol clave en el cumplimiento de SOX, ya que:

- Procesan transacciones financieras.
- Consolidan información contable.
- Generan reportes financieros.
- Almacenan evidencia histórica de operaciones.

Desde TI, SOX impacta principalmente en los llamados **IT General Controls – ITGC (Controles Generales de Tecnología de la Información)**, que aseguran que los sistemas funcionen de manera controlada y predecible.

Estos controles no validan cifras contables, sino **el entorno tecnológico que las produce**.

---

3. Principales áreas de impacto de SOX en TI

Desde la mirada de los sistemas y tecnologías de la información, SOX exige especial atención en las siguientes áreas:

---

a) Control de accesos (Access Controls – Controles de Acceso)

SOX requiere que solo personas autorizadas puedan acceder a sistemas que procesan información financiera.

Desde TI, esto implica:

- Gestión de usuarios y perfiles.
- Separación de funciones (**Segregation of Duties – Segregación de Funciones**).
- Registro de accesos y actividades.

Ejemplo: un usuario que registra transacciones no debería poder aprobarlas ni modificar reportes financieros.

---

b) Gestión de cambios (Change Management – Gestión de Cambios)

Todo cambio en sistemas que impacten información financiera debe estar **formalmente autorizado, documentado y probado**.

Desde TI:

- Se deben registrar cambios en aplicaciones, bases de datos e infraestructura.
- Deben existir ambientes separados (desarrollo, prueba y producción).
- Se debe garantizar la trazabilidad del cambio.

Ejemplo: una modificación en el cálculo de impuestos dentro de un ERP debe estar aprobada y documentada.

---

c) Operación y continuidad de los sistemas (IT Operations – Operaciones de TI)

SOX exige que los sistemas críticos estén disponibles y funcionen de manera confiable.

Desde los sistemas de información:

- Se requieren respaldos (**Backups – Copias de Seguridad**).
- Planes de continuidad (**BCP – Business Continuity Plan / Plan de Continuidad del Negocio**).
- Planes de recuperación ante desastres (**DRP – Disaster Recovery Plan / Plan de Recuperación ante Desastres**).

d) Integridad y trazabilidad de la información (Data Integrity – Integridad de los Datos)

Los datos financieros deben ser completos, exactos y no alterables sin control.

Desde TI:

- Se implementan controles de validación.
- Se mantienen logs y auditorías de transacciones.
- Se evita la manipulación no autorizada de datos.

---

4. Sección 404 de SOX y su impacto en TI

Uno de los artículos más relevantes de la ley es la **Sección 404**, que exige que la dirección:

- Evalúe la efectividad de los controles internos.
- Certifique formalmente su funcionamiento.
- Sea responsable ante fallas significativas.

Desde TI, esto implica que los responsables tecnológicos:

- Deben documentar procesos y controles.
- Participan activamente en auditorías internas y externas.
- Son corresponsables del cumplimiento regulatorio.

La tecnología deja de ser un área puramente operativa para convertirse en un **actor clave del gobierno corporativo**.

---

5. Relación de SOX con otros marcos de referencia

En la práctica, SOX no se implementa de forma aislada. Las organizaciones suelen apoyarse en frameworks como:

- **COBIT (Control Objectives for Information and Related Technologies – Objetivos de Control para la Información y las Tecnologías Relacionadas)** para estructurar controles de TI.
- **ITIL (Information Technology Infrastructure Library – Biblioteca de Infraestructura de TI)** para la gestión operativa.

- **ISO/IEC 27001** para seguridad de la información.

Desde la administración, estos marcos facilitan demostrar cumplimiento y ordenar los procesos tecnológicos exigidos por SOX.

---

6. Ejemplo aplicado a una organización

Una empresa que cotiza en bolsa utiliza un **ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales)** para su contabilidad.

Para cumplir con SOX desde TI:

- Define perfiles de acceso estrictos.
- Documenta y aprueba cada cambio en el sistema.
- Registra auditorías de transacciones.
- Implementa respaldos y controles de continuidad.

El cumplimiento de SOX no depende solo del área contable, sino del **correcto funcionamiento del sistema de información**.

Conclusión

La **Sarbanes-Oxley Act (SOX)** ha convertido a los **Sistemas y Tecnologías de la Información** en un componente central del **control interno y la confiabilidad de la información financiera**. Desde la mirada de la administración, SOX demuestra que la tecnología no es un soporte neutro, sino un **factor crítico de riesgo y cumplimiento regulatorio**.

Para los estudiantes de licenciatura en administración, comprender SOX desde TI implica reconocer que la gestión de sistemas de información tiene **implicancias legales, financieras y estratégicas**. Un sistema mal controlado puede comprometer la credibilidad de la información financiera y exponer a la organización a sanciones significativas. En este sentido, SOX refuerza la necesidad de integrar **gobernanza, control y tecnología** como partes inseparables de la gestión organizacional moderna.

Preguntas de autoevaluación

1. ¿Cuál es el objetivo principal de la Ley Sarbanes-Oxley?

2. ¿Por qué los sistemas de información son críticos para el cumplimiento de SOX?
3. ¿Qué son los IT General Controls (ITGC) y por qué son relevantes?
4. ¿Cómo impacta la Sección 404 de SOX en el área de TI?
5. ¿Qué riesgos organizacionales surgen si los sistemas financieros no están adecuadamente controlados?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.